Exercise 3 – Sikkerhet og kryptografi

Capture-the-flag challenge

**Type of challenge**: Code injection

**Technical details:**

Docker-compose .yaml file used for defining the Docker-application, where php is specified as the service that the application will run. The port is specified as localhost listening on port 5001 (host machine) which is connected to the docker-container at port 80.

The Dockerfile is custom-made and specifies the docker-image used (php:7.4-apache) and some initial commands to set up the environment. The dump\_io module is used for picking up the content in POST-variables.

The PHP-application that is being run in the docker-container is a simple validation form where you are asked to fill in your name, email, website, comments and select a gender.

**How to solve:**

The challenge is meant to be solved by trying to use code injection in the input-fields before you submit them. Most of the input-fields will remove symbols used for code injection, so they will have to try on all of the fields before finding the one that works. If the code injection is done in the correct input-field you are presented with the Flag, which can be inserted into the comment-field to receive a special surprise.

**Hints:** Some of the input-fields are not as well secured as others.

**Difficulty:** Easy

**Knowledge required:** Basic knowledge on code injection

**Resources necessary:** Docker, Docker-compose

**Instructions for building:**

1. Unzip the challenges.zip where you want to store the application
2. Navigate to the location where you unzipped the directory through your terminal
3. Run command: docker-compose up (this runs the containers). Add -d to run containers in the background
4. Run command: docker-compose logs -f to follow along the logs for the application (includes content in POST-variables – which is used when submitting form)
5. Go to any browser and enter localhost:5001 in the URL
6. Finished!